Notice of Allowability	Application No.	Applicant(s)	
	09/940,083	FELDMAN ET AL.	
	Examiner	Art Unit	
	Bradley B. Bayat	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/27/2005*.

2. ☒ The allowed claim(s) is/are *20,22-25 and 28-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Prior office actions are hereby incorporated by reference. Applicant's 132 Affidavit by the inventor is hereby acknowledged and entered. The terminal disclaimer submitted has been entered into the record.

- Claims 1-19, 21, 26 27 and 31 have been canceled.
- Claims 20 and 30 have been amended.
- Claims 20, 22-25 and 28-30 have been allowed.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an interview with applicant's attorney. As per our conversation, Claims 20, 22-25 and 28-30 have been amended. The attorney of record should contact the examiner if there is any inconsistency or discrepancy with regards to this action.

The claims in the application has been amended as follow:

20. (Currently Amended) A storage device comprising:

- a computer readable storage medium; and

- a computer executable storage engine, the storage engine configured to generate a secure session key and to receive encrypted content and a corresponding encrypted content key from a host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium, wherein the storage medium is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system.

21. CANCELLED.

22. (Previously Presented) The storage device of claim 20, wherein the storage engine is further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure session key only by decrypting the encrypted secure session key using the private key corresponding to the public key.

23. (Previously Presented) The storage device of claim 22, wherein the storage engine is further configured to doubly-encrypt the encrypted content using at least a second storage engine encryption key.

24. (Previously Presented) The storage device of claim 23, wherein the second storage engine encryption key comprises a Data Encryption Standard (DES) key.

25. (Previously Presented) The storage device of claim 24, wherein the DES key comprises a triple DES key.

26. CANCELLED.

27. CANCELLED.

28. (Previously Presented) The storage device of claim 22, wherein the public key and the private key are elliptic curve cryptography keys.

29. (Previously Presented) The storage device of claim 20, wherein the storage engine includes a random number generator for generating the secure session key.

30. (Previously Presented) A method of writing to a storage device from a host system having a public key and a corresponding private key, comprising:

- encrypting a secure session key using the public key;
- recovering the secure session key from the encrypted secure session key using the corresponding private key;

- encrypting content according to a content key and commanding the storage device to write the encrypted content to a storage medium;
- encrypting the content key using secure session key and transmitting the encrypted content key to the storage device; and
- in the storage device, decrypting the encrypted content key using the secure session key.

31. CANCELLED.

Allowable Subject Matter

Claims 20, 22-25 and 28-30 are allowed over the prior art of record.

The closest prior art of record is US 6,636,966 B1 by applicant Lee et al. and Ansell et al, 6,367,019 B1.

The closest prior art of record, Ansell et al., fails to disclose a storage engine based DRM scheme. Particularly, the storage engine and method of claims 20 and 30 are configured to encrypt the decrypted content key with a first storage engine key and to write the storage engine encrypted key to the storage medium, rather than the host. The pertinent portion of claim 20 recites: a computer executable storage engine, the storage engine configured to generate a secure session key and to receive encrypted content and a corresponding encrypted content key from a host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium, wherein the storage medium is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature

provided by the host system. Thus, the storage engine encryption key never leaves the storage engine, which makes it more secure than the host system disclosed by Ansell et al. Dependent claims 22-25, 28 and 29 are allowable for the foregoing reasons.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.

bbb

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600